ABSTRAK

Untuk menunjang keamanan suatu *website* dalam melindungi informasi pengguna, dibutuhkan suatu sistem keamanan seperti *SSL (Secure Socket Layer)* agar semua informasi pengguna yang diakses melalui *website* tersebut tidak terbaca oleh pihak yg tidak berwenang.

Belakangan ini ditemukan bugs bernama Heartbleed, bugs ini terdapat pada fitur *Heartbeat* pada *SSL (Secure Socket Layer)*, fungsi dari *Heartbeat* ini adalah menjaga *session connectivity* antara komputer server dan client. Pada penelitian tugas akhir ini, penulis melakukan pengujian terhadap *SSL (Secure Socket Layer)* yang dipakai SITU FT unpas. Pengujian ini bertujuan untuk mengetahui apakah *SSL (Secure Socket Layer)* yang dipakai SITU FT Unpas mampu menjaga keamanan informasi pengguna.

Jika dinyatakan *SSL (Secure Socket Layer)* yang dipakai SITU FT Unpas tidak mampu melindungi informasi pengguna, maka penulis akan melakukan implementasi dengan *SSL (Secure Socket Layer)* yang lain. Berdasarkan *OpenSSL.org, OpenSSL v 1.0.2* dinyatakan mampu mencegah *Bugs Heartbleed.*

Setelah penulis melakukan implementasi *OpenSSL v 1.0.2*, penulis akan melakukan pengujian ulang dengan metode yang sama untuk melihat apakah *OpenSSL* yang telah diimplementasikan mampu mecegah *Bugs Heartbleed*.

Kata kunci: *Heartbleed, SSL, OpenSSL*

ABSTRACT

In order to support website security in protecting user's information, a security system like SSL (Secure Socket Layer) is needed so that all users' information accessed through a website can't be read by unauthorized parties.

A bug called Heartbleed was recently found, it's on the Heartbeat's features in SSL (Secure Socket Layer), Heartbeat has function to protect the session connectivity between computers and client. At this research, the author tests the SSL (Secure Socket Layer) used by SITU FT Unpas. This test aims to find out whether the SSL (Secure Socket Layer) used by SITU FT Unpas is able to protect users' information.

If the SSL (Secure Socket Layer) used by SITU FT Unpas is not able to protect users' information, another SSL (Secure Socket Layer) will be implemented. Based on OpenSSL.org, OpenSSL v 1.0.2 is said to be able to prevent Heartbleed Bugs.

After the author implemented the OpenSSL v.1.0.2, retesting will be performed using the same method to find whether the implemented OpenSSL is able to prevent Heartbleed Bugs.

Keyword: *Heartbleed, SSL, OpenSSL*